

## Office of Information Technology Policy

## Modem Use

---

**Purpose:**

Network security is enhanced by eliminating or removing unnecessary access points to the internal network. Modems on network-attached personal computers essentially circumvent the enterprise firewall system by creating additional unguarded entry points to the internal network. Hackers often exploit this vulnerability to gain access to the internal secure network.

**Policy:**

Modem hardware attached to or installed in desktop computer systems connected to the network is prohibited. Additionally, laptop users are prohibited from using simultaneous connections via the modem and the network interface.

**Scope:**

This policy applies to all entities under the authority of the Office of Information Technology pursuant to the provisions of R.S. 39:15.1, et seq. Agencies in compliance with this policy will prevent employees from establishing network connections that may jeopardize the security of internal networks and network assets. Relative to network-attached desktop personal computers, best practices indicate that network security is enhanced by the removal of modems.

**Responsibilities:**

Agencies must establish policies and procedures to:

- Ensure all internal/external modem hardware is removed from network-attached desktop computers.
- Prohibit the installation and use of modem hardware in network-attached desktop computers.
- Govern the use of laptop computers.
- Periodically verify compliance with this policy.

Agencies should develop policies and procedures to address modem use relative to other computer hardware platforms (server, mid-range, mainframe, etc.).

**Effective Date:**

January 27, 2003

Reissued May 1, 2003 (revised scope statement)

## Office of Information Technology Policy